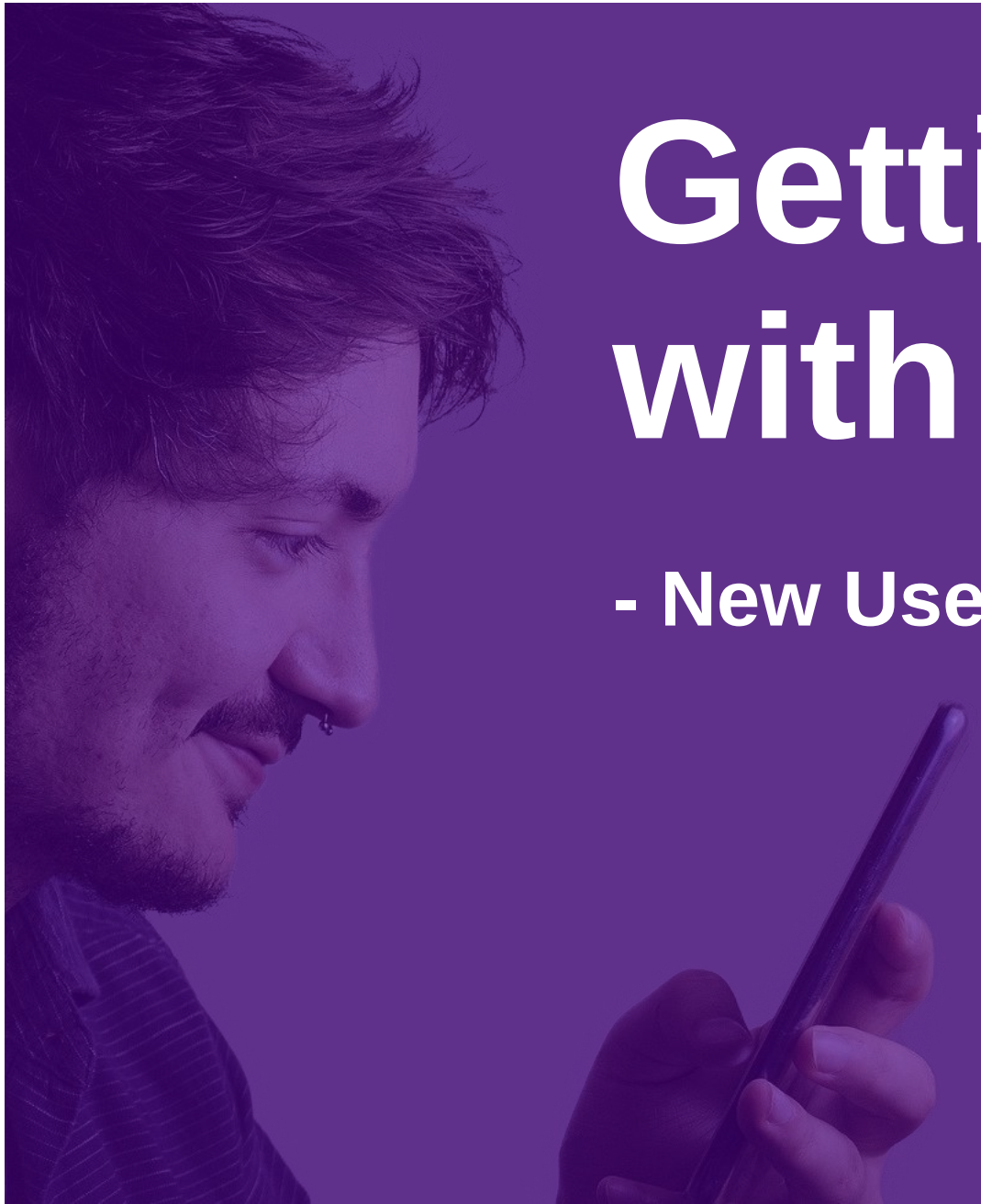
Tampere University
Tampere University of Applied Sciences



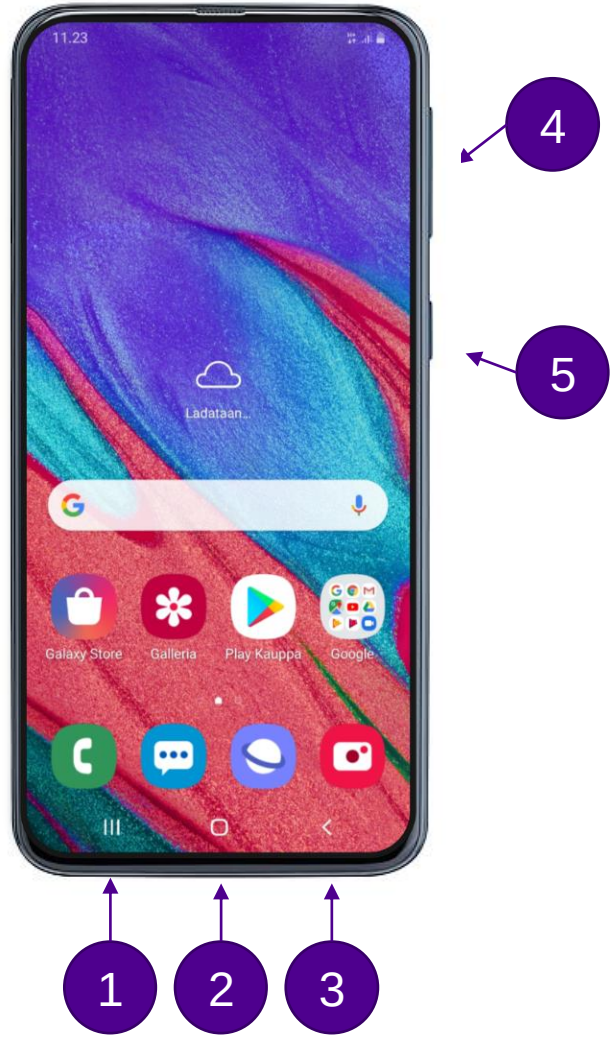
Getting started with your phone

- New User

Basics of Samsung Galaxy mobile phone (1/2)

The control buttons appear when the screen is active:

1. Last used applications
2. Home button
3. Back button
4. Volume control
   - press down to change the phone mode to silent
   - the volume during the call can be adjusted
5. Power key / Lock key - To turn on the device press and hold the power key



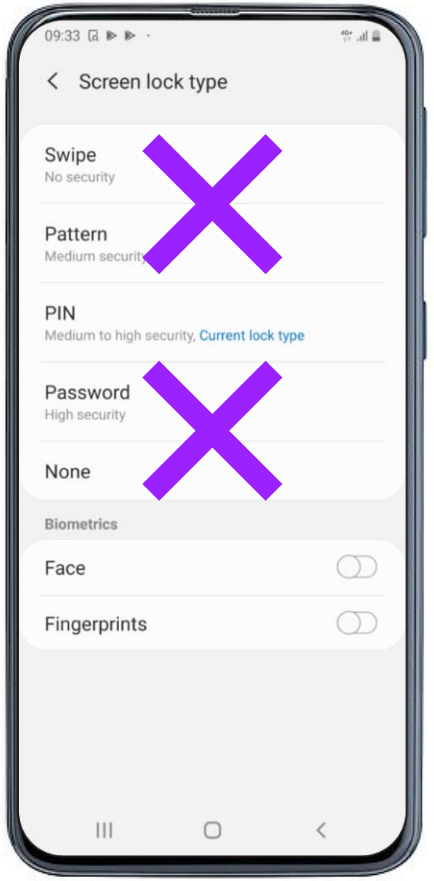
Basics of Samsung Galaxy mobile phone (2/2)

- Icons and widgets can be edited on the bottom navigation bar and home screens by tapping your finger over the icon, widget or empty space. By "pinching" the screen you can add and remove the home screens.
- Swipe from bottom to top to see all the applications installed on your device.
- Swipe down from the top (example image) to see quick settings (eg wlan, bluetooth) and the latest notifications (emails, messages, calls).

Security / Adding a screen lock code

By setting a screen lock code on your device, it will protect the information on your device in case your phone is lost or stolen. Without a security code, the finder has access to e.g. all your emails and other information on your device. You can also use your fingerprint to unlock your phone.

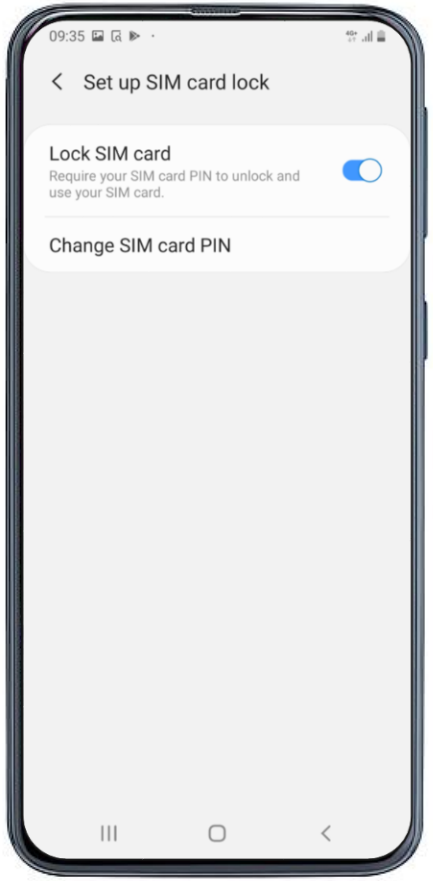
- Swipe down from the top to see the shortcut menu
- Select the settings icon from the top right
- Select *Lock screen*
- Select *Screen lock type*
- **Select *PIN (at least 6 numbers)***
- Enter the desired PIN twice
  - the PIN must not be too easy to find out



Security / Changing the PIN code of the SIM card

The default PIN code for Elisa's line is 1234. This should be replaced.

- Swipe down from the top to see the shortcuts menu
- Select the settings icon from the top right
- Click *Biometrics and security*
- Select *Other security settings*
- Select *Set up SIM card lock*

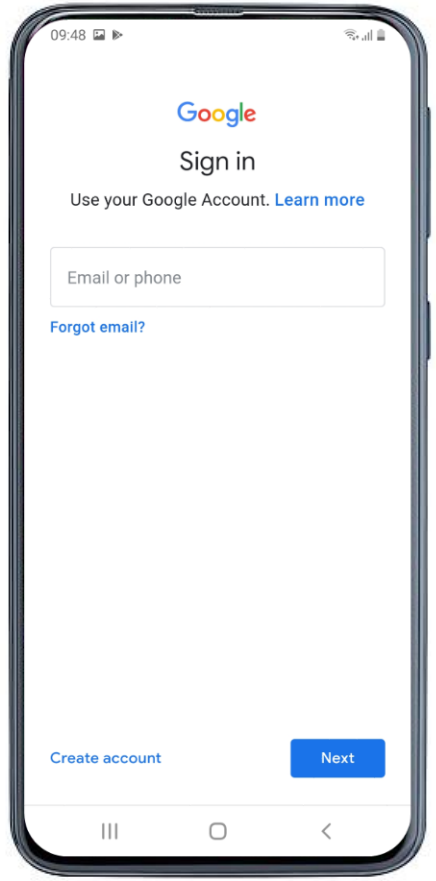


Accounts / Adding Google account

A Google Account allows you to install new applications and keep your device up to date and safe to use.

- Swipe down from the top to see the shortcuts menu
- Select the settings icon from the top right
- Select *Accounts and backup* > *Accounts* > *Add account* > *Google*
- You can use your existing Gmail address or, alternatively, create a new Google account e.g. firstname.surname.tuni@gmail.com

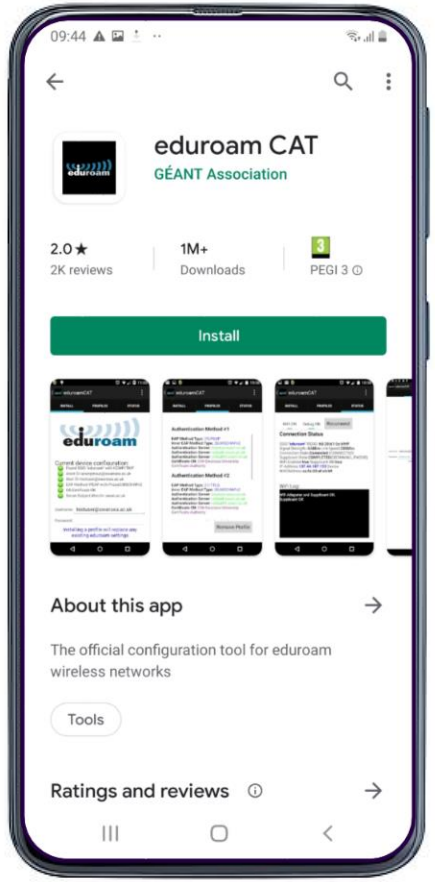
- **Note** that if you use the same personal Google account in your business phone as your own phone, the account may import a personal calendar, contacts, and try to install apps on your work phone → **It is recommended that you create a new Google account for your work phone.**



Network / Adding Eduroam (WiFi)

With Eduroam network your phone uses the Wi-Fi of Tampere universities and other universities for network traffic instead of a data connection by the phone operator.

- Install the “geteduroam” application from the Play Store
- Open the "geteduroam" application
- Select Tampere Universities
- Enter your TUNI email address in the username field
- Enter your TUNI password in the password field
- Wireless networks



Setting up multifactor authentication

- **The electronic services of the university community require multifactor authentication.**
- Multifactor authentication (MFA) involves an additional authentication on your mobile phone when logging in to cloud services. MFA adds an extra layer of security to your account when you log in to the TUNI electronic services, especially if your password has ended up in the wrong hands.
- The use of MFA is free of charge and only requires a phone that is connected to the intranet and can be equipped with the Microsoft Authenticator app that is available for download on Android and Apple phones.
- **If you prefer not to download the app, you have the option to enable SMS-based MFA.** However, the authenticator app is **recommended** due to its ease of use.
- You can install the Microsoft Authenticator app on multiple phones and use it when logging into to other personal services, such as Google services.
- **Setting up TUNI multifactor authentication**

Mobile Device Management

- **What is Mobile Device Management?**
  - Microsoft Intune Mobile Device Management (MDM) is a solution that helps to improve information security in mobile phones, tablet computers and the information systems used by the Universities community. The solution consists of an app running on a mobile device and a management system running on a cloud service.
  - The solution is available to Android, iPhone, and iPad devices.
- **MDM must be deployed on all mobile devices owned by the employer.**
- More info and instructions

Useful links for using your TAMK or University issued mobile phone

- Use of mobile phones
- Use of mobile phones abroad
- Mobile phone and data plans
- Information security and mobile phones

Tampere University
Tampere University of Applied Sciences

Need more information?

- it-helpdesk@tuni.fi
- 0294 520 500